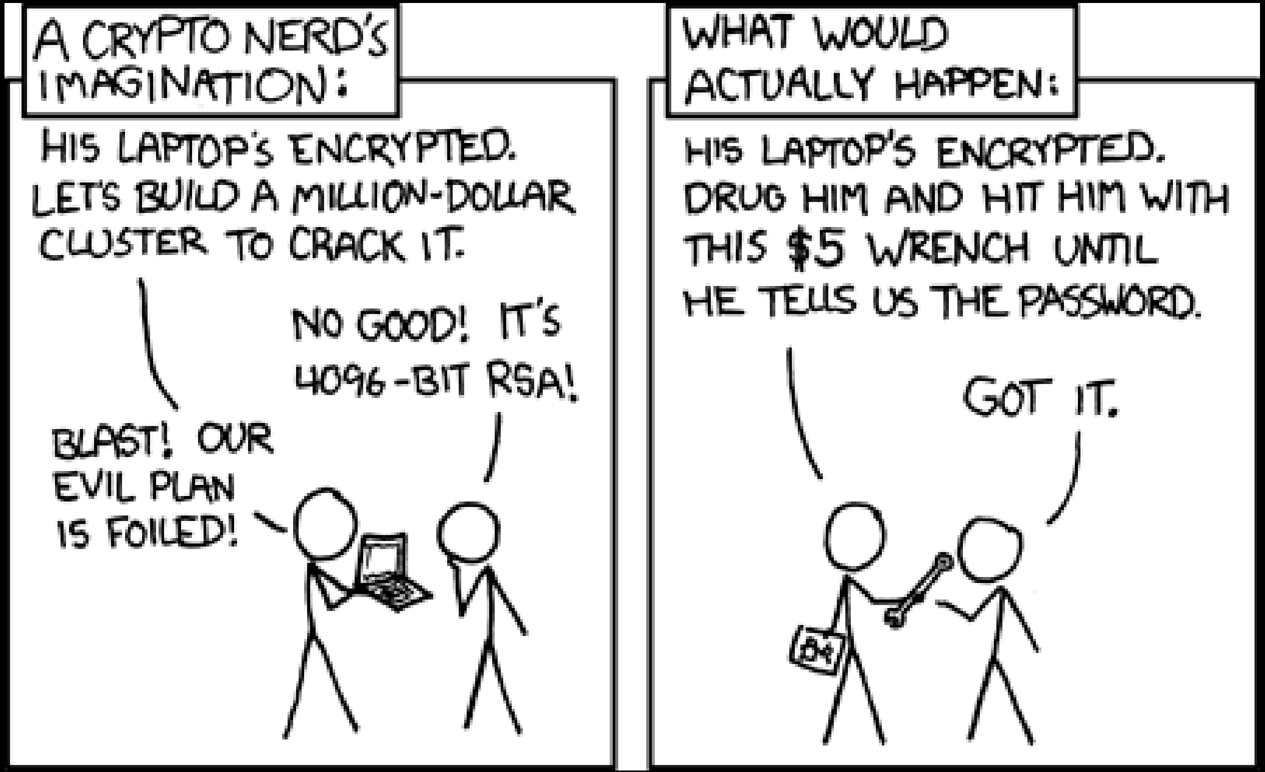
Security Design & High-Risk Users

Eleanor Saitta @Dymaxion

HITB GSEC 2015


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Security is not about computers.

People built computers to accomplish tasks.

People built more computers and networked them to accomplish more tasks.

Those computers got compromised.

People paid us to fix the problem.

We made the mistake of thinking they meant us to fix the computers.

Having made this mistake, we built an entire industry around solving the wrong problem.

People built yet more computers and networks.

We realized we couldn’t secure them individually and started looking at probabilities and scaling.

We never did fix the problem.

Security is the set of activities that reduce the likelihood of a set of adversaries successfully frustrating the goals of a set of users.

The ability to define and determine what a technical system will and will not do is necessary but not sufficient to determine whether it is secure.

Defining security for a system means understanding what your humans want.

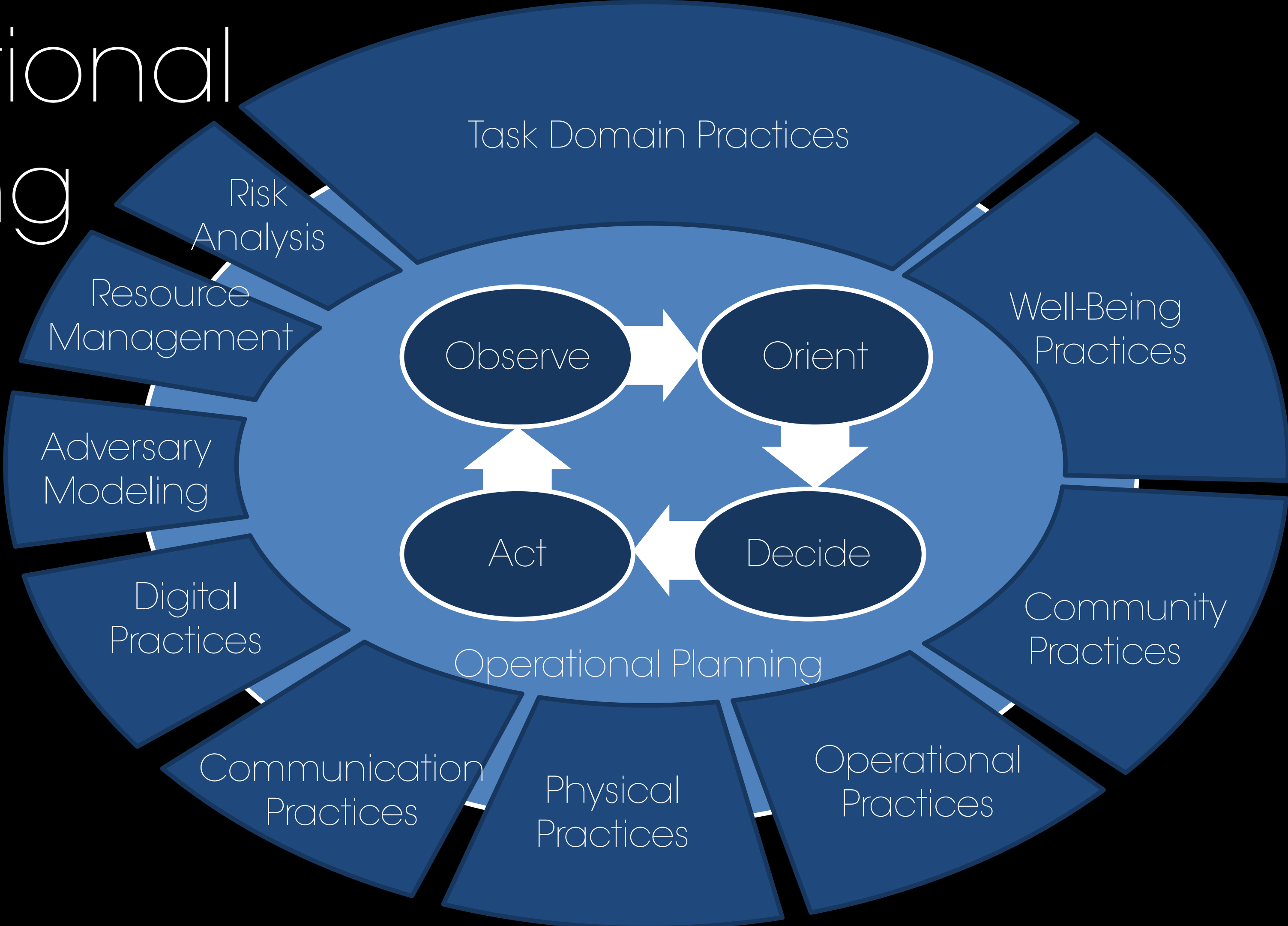
Security design is the process of understanding user culture, goals, and workflows, organizational technical capabilities, and adversary capabilities and dispositions and synthesizing a satisficing solution.

Outcomes are messy

Understanding the Operations Process

- Planning in the presence of an adversary
- OODA Loops
- Cognitive overhead
- Operational utility
- Functional deployability

Operational Planning



Worse

Efficacy

is

Better

Invariants

Availability

Confidentiality

Deployability

Efficacy

Integrity

Interoperability

Nonrepudiation

Simplicity

Trust

Unlinkability

Invariants

Accuracy

Adaptability

Agility

Anticipation

Assurance

Availability

Awareness

Capacity

Coherence

Concealment

Confidentiality

Continuity

Control

Completeness

Cooperation

Coordination

Deception

Deployability

Deniability

Depth

Deterrence

Discipline

Dispersion

Economy

Efficacy

Endurance

Exposure

Identifiability

Initiative

Integration

Integrity

Interoperability

Goodwill

Mobility

Nonrepudiation

Objectivity

Precision

Predictability

Readiness

Receptivity

Redundancy

Relevancy

Resilience

Responsiveness

Simplicity

Simultaneity

Surprise

Survivability

Synchronization

Trust

Timeliness

Susceptibility

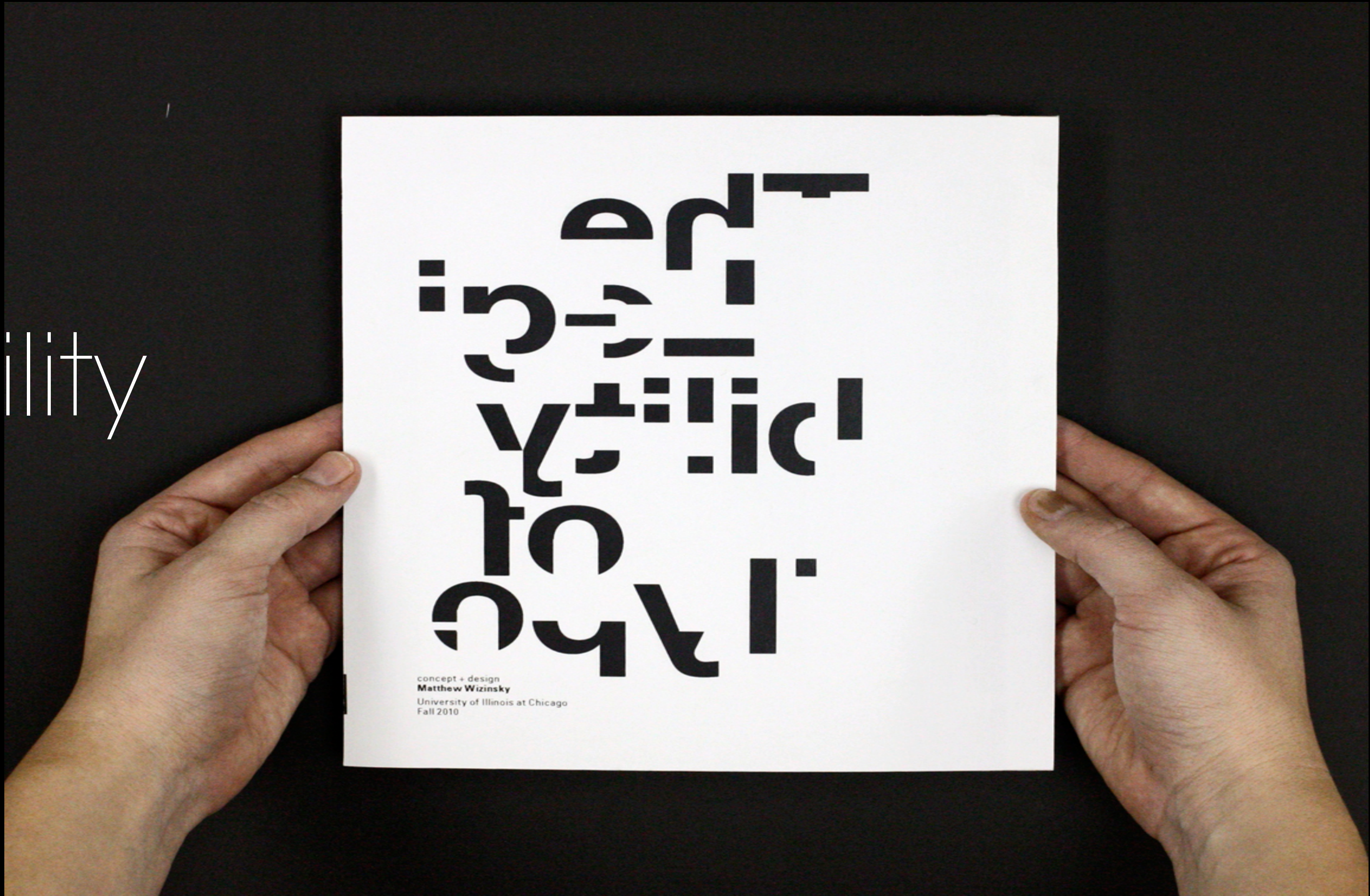
Uncertainty

Unlinkability

Unpredictability

Velocity

Legibility


concept + design
Matthew Wizinsky
University of Illinois at Chicago
Fall 2010

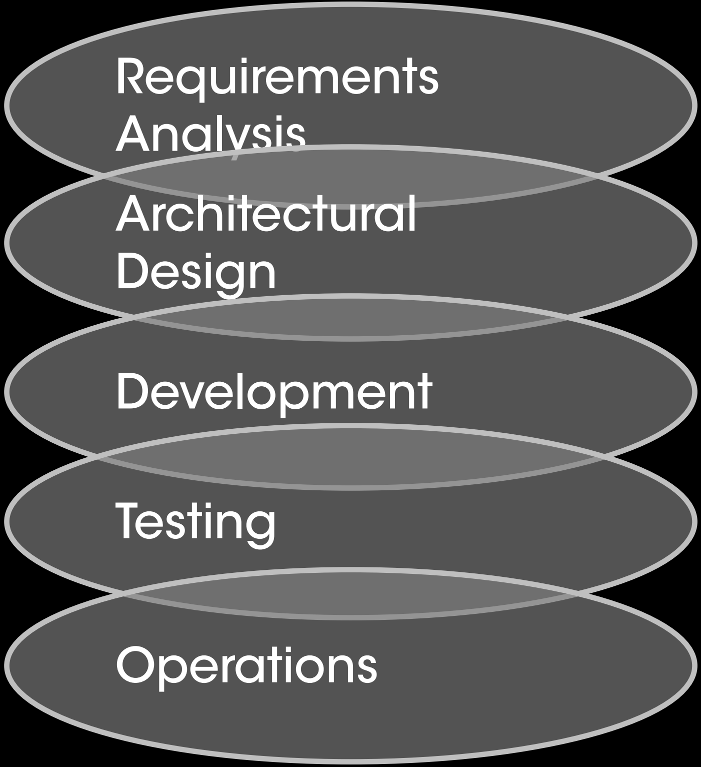
Design

- Understanding, documenting, and communicating constraints and capabilities
- Synthesize and validate potential solutions
- Communicate and justify those solutions
- Support the development process & prevent drift

Participatory Design

- Recognize users as authorities on their goals
- Deep cultural engagement for complex scenarios
- Surface tacit and embodied knowledge
- Build long-term community trust
- Short-circuit long development processes
- Create blended countermeasures
- Minimize team ego

Mapping the Security Task



Requirements Analysis

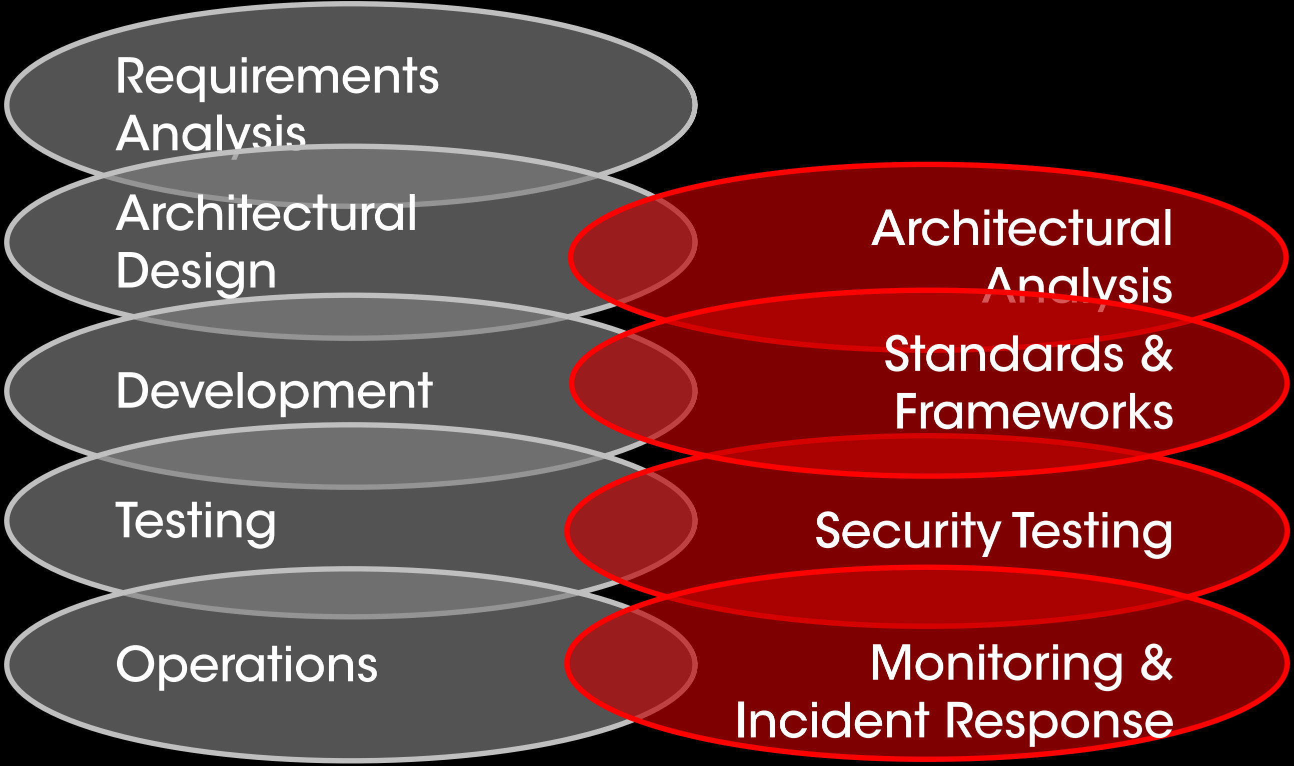
Architectural Design

Development

Testing

Operations

Mapping the Security Task



Requirements Analysis

Architectural Design

Development

Testing

Operations

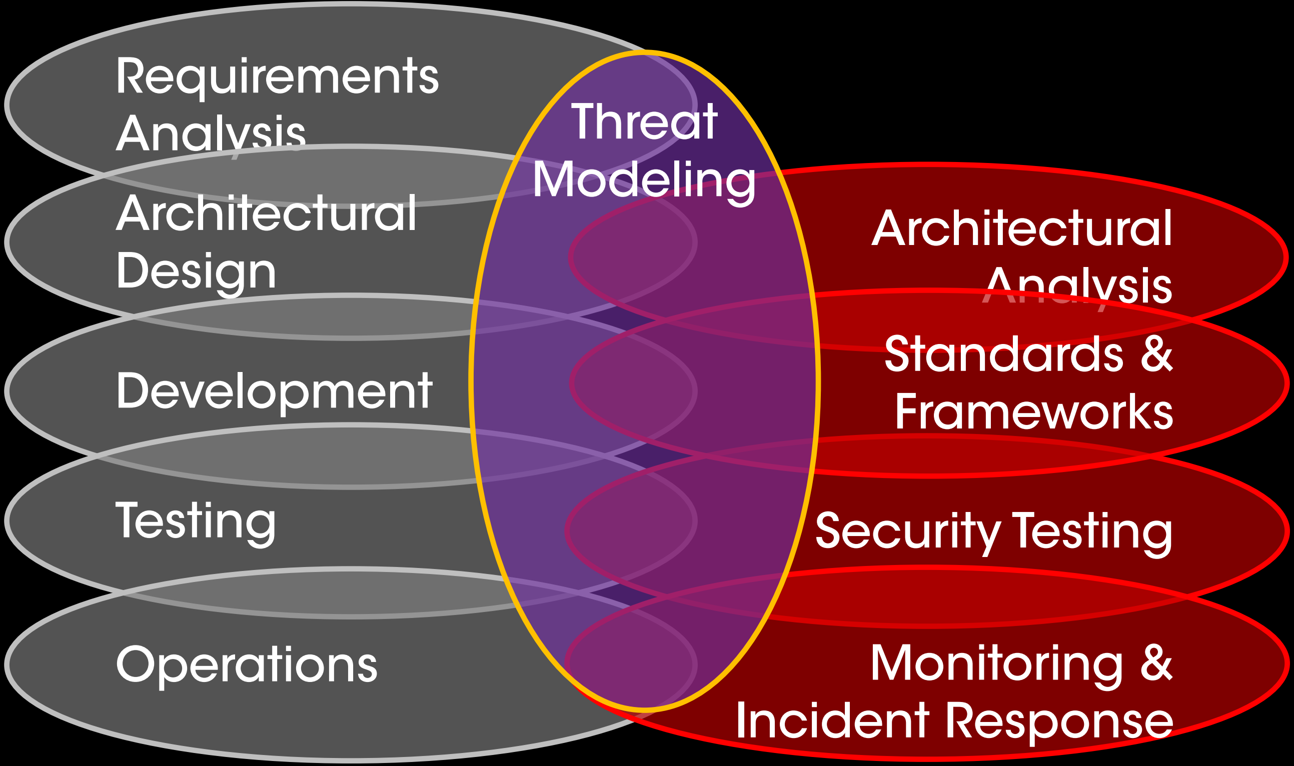
Architectural Analysis

Standards & Frameworks

Security Testing

Monitoring & Incident Response

Mapping the Security Task



Requirements Analysis

Architectural Design

Development

Testing

Operations

Threat Modeling

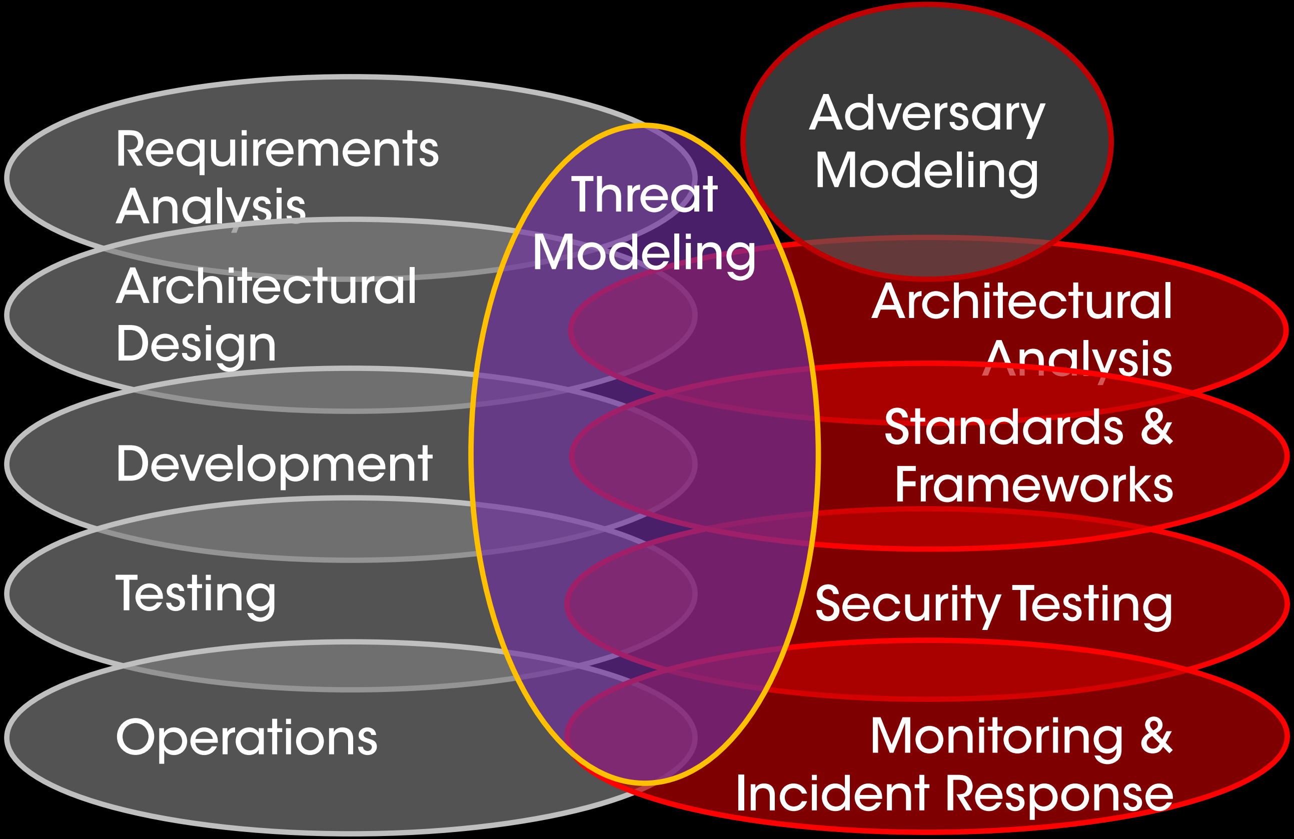
Architectural Analysis

Standards & Frameworks

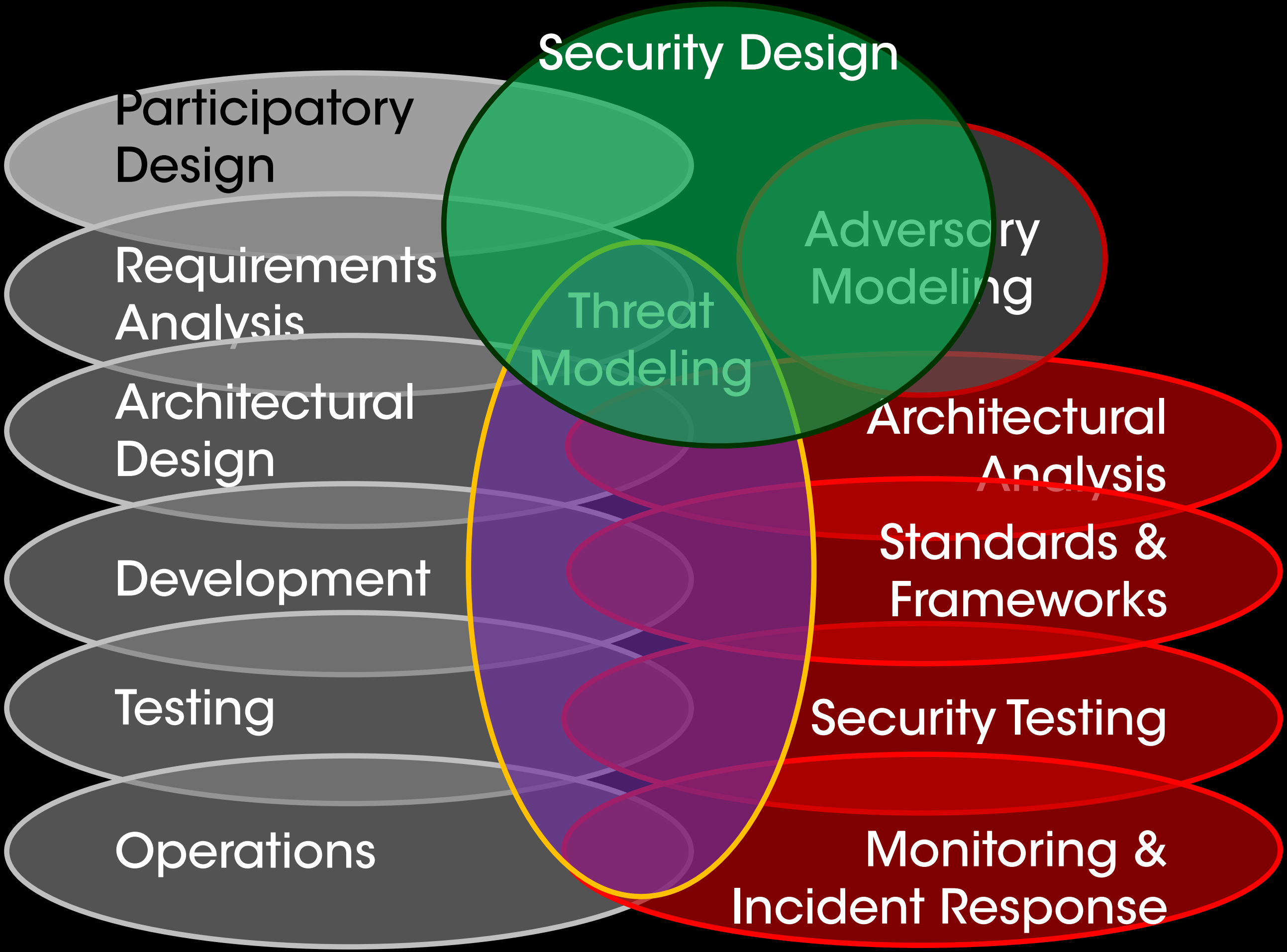
Security Testing

Monitoring & Incident Response

Mapping the Security Task



Mapping the Security Task



Practical Process Change

- Find your UX designers and product managers
- Insist on coming to all of their meetings
- Learn their language and process
- Learn what your users are actually trying to do
- Design requirements-level security support
- Document and solidify once you have results
- Give yourself room to fail
- Work across your org to center user goals

Thank you!

http

ella@dymaxion.org

twitter

Support my security research and writing:

http://patreon.com/dymaxion